Title : Rekeying in Secure Mobile Multicast Communications

Abstract

A method of inter-area rekeying of encryption keys in secure mobile multicast communications, in which a Domain Group Controller Key Server (Domain GCKS) distributes Traffic Encryption Keys (TEK) to a plurality of local Group Controller Key Servers (local GCKS), and said local Group Controller Key Servers forward said Traffic Encryption Keys, encrypted using Key Encryption Keys (KEK_i, KEK_j) that are specific to the respective local Group Controller Key Server (local $GCKS_i$, $GCKS_j$), to group members, said local Group Controller Key Servers ($GCKS_i$, $GCKS_j$) constituting Extra Key Owner Lists ($EKOL_i$, $EKOL_j$) for group key management areas ($area_i$, $area_j$) that distinguish group members (MM_i, MM_j) possessing Key Encryption Keys (KEK_i, KEK_j) and situated in the corresponding group key management area ($area_i$, $area_j$) from group members (MM_{ij}) possessing Key Encryption Keys (KEK_i) that were situated in the corresponding group key management area ($area_i$) but are visiting another area ($area_j$).